INSTITUTE FOR DEFENSE ANALYSES

Assured Identity for Enterprise Level Security

William R. Simpson

Kevin E. Foltz

July 11, 2017

IDA Non-Standard
NS D-8286
Log:
H 2016-001325
Copy

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task BC-5-2283, "Architecture, Design of Services for Air Force Wide Distributed Systems," for USAF HQ USAF SAF/CIO A6. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

For more information:

William R. Simpson, Project Leader
rsimpson@ida.org, 703-845-6637

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Assured Identity for Enterprise Level Security

William R. Simpson and Kevin E. Foltz

***Abstract* — Increasing threat intrusions to enterprise computing systems have led to a formulation of guarded enterprise systems. The approach was to put in place steel gates and prevent hostile entities from entering the enterprise domain. The current complexity level has made the fortress approach to security implemented throughout the defense, banking, and other high-trust industries unworkable. The alternative security approach, called Enterprise Level Security (ELS), is the result of a concentrated 14-year program of pilots and research. The primary identity credential for ELS is the PKI certificate, issued to the individual who is provided with a Personal Identity Verification (PIV) card with a hardware chip for storing the private key. All sessions are preceded by a PKI mutual authentication, and a TLS 1.2 communication pipeline is established. This process was deemed to provide a high enough identity assurance to proceed. However, in some instances the PIV card is not available and a compatible approach is needed. This paper discusses a multi-level authentication approach designed to satisfy the level of identity assurance specified by the data owner and to be compatible with the ELS approach for security.**

***Index Terms* — Identity, Authentication, Multi-Factor Authentication, Enterprise Level Security**

I. INTRODUCTION

Adversaries continue to penetrate, and in many cases, already exist within, our network perimeter, i.e., they have infiltrated the online environment, jeopardizing the confidentiality, integrity, and availability of enterprise information and systems. The fortress model – hard on the outside, soft on the inside – assumes that the boundary can prevent all types of penetration [8], but this assumption has been proven wrong by a multitude of reported network-related incidents. The previous statements are no longer controversial but a wise assumption for data and information security practitioners. Network attacks are pervasive, and nefarious code is present even in the face of system sweeps to discover and clean readily apparent malware. The focus of this paper is on the security aspects of countering existing known and unknown threats based on robust identity and access management (IdAM) and on how this access control system can dynamically support mission information requirements. A working prototype has been developed and evaluated for security, functionality, and scaling issues. Due to space constraints, multi-level security issues are not addressed in this paper.

Manuscript received 12 February 2017; revised 14 March 2017. This work was supported in part by the U.S. Secretary of the Air Force and The Institute for Defense Analyses (IDA). The publication of this paper does not indicate endorsement by any organization in the Department of Defense or IDA, nor should the contents be construed as reflecting the official position of these organizations

Kevin E. Foltz is with the Institute for Defense Analyses. (email: kfoltz@ida.org).

William R. Simpson is with the Institute for Defense Analyses, 4850 Mark Center Drive, Alexandria, Virginia 22311 USA, and is the corresponding author phone: 703-845-6637, FAX: 703-845-6848 (e-mail: rsimpson@ida.org).

Enterprise Level Security (ELS) is a capability designed to counter adversarial threats by protecting applications and data with a dynamic claims-based access control (CBAC) solution. ELS helps provide a high-assurance environment in which information can be generated, exchanged, processed, and used. It is important to note that the ELS design is based on a set of high-level tenets that are the overarching guidance for every decision made, from protocol selection to product configuration and use [7]. From there, a set of enterprise-level requirements are formulated that conforms to the tenets and any high-level guidance, policies, and requirements.

The basic tenets, used at the outset of the ELS security model, are the following:

0. Malicious entities are present.
1. Simplicity.
2. Extensibility.
3. Information hiding.
4. Accountability.
5. Specify Minimal detail.
6. Service-driven rather than a product-driven solution.
7. Lines of authority should be preserved.
8. Need-to-share as overriding need-to-know.
9. Separation of function.
10. Reliability.
11. Trust but verify (and validate).
12. Minimum attack surface.
13. Handle exceptions and errors.
14. Use proven solutions.
15. Do not repeat old mistakes.

The current paper-laden access control processes for an enterprise operation are plagued with ineffectiveness and inefficiencies. In a number of enterprises, tens of thousands of personnel transfer locations and duties annually, which on a daily basis introduces delays and security vulnerabilities into their operations. ELS mitigates security risks while eliminating much of the system administration required to manually grant and remove user/group permissions to specific applications/systems. Early calculations show that for government and defense, 90–95% of recurring man-hours will be saved and up to 3 weeks in delay for access request processing will be eliminated by ELS-enabled applications [11]. While a perimeter-based architecture assumes that threats are stopped at the front gates, ELS does not accept this precondition and is designed to mitigate many of the primary vulnerability points at the application using a distributed security architecture, shown in Figure 1.

II. ENTERPRISE LEVEL SECURITY

The ELS design addresses five security principles that are derived from the basic tenets:

- Know the Players – this is done by enforcing bi-lateral end-to-end authentication;
- Maintain Confidentiality – this entails end-to-end unbroken encryption (no in-transit decryption/payload inspection);
- Separate Access and Privilege from Identity – this is done by an authorization credential;
- Maintain Integrity – know that you received exactly what was sent;
- Require Explicit Accountability – monitor and log transactions.

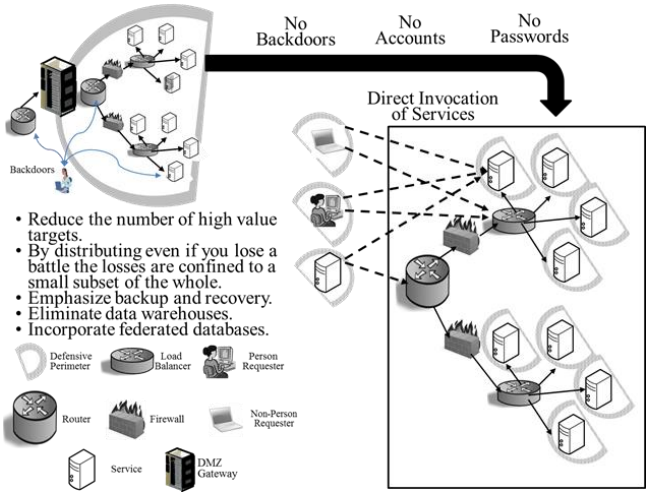

Figure 1: Distributed Security Architecture

A. Know the Players

In ELS, the identity certificate is an X.509 Public Key Infrastructure (PKI) certificate [1]. This identity is required for all active entities, both person and non-person, e.g., services, as shown in Figure 2. PKI certificates are verified and validated. Ownership is verified by a holder-of-key check. Supplemental (in combination with PKI) authentication factors may be required from certain entities, such as identity confirming information or biometric data.

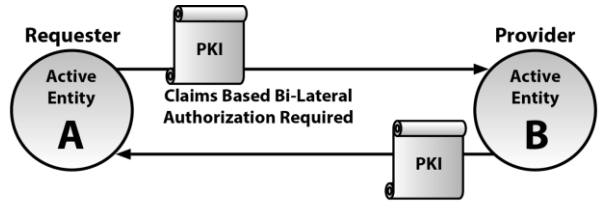

Figure 2: Bi-lateral Authentication

B. Maintain Confidentiality

Figure 3 shows that ELS establishes end-to-end Transport Layer Security (TLS) [2] encryption (and never gives away private keys that belong uniquely to the certificate holder).

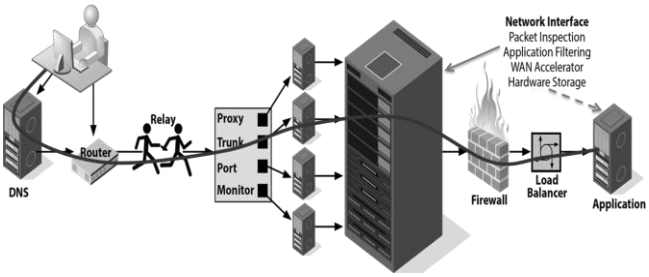

Figure 3: End-to-End Encryption

C. Separate Access and Privilege from Identity

ELS can accommodate changes in location, assignment, and other attributes by separating the use of associated attributes from the identity. Whenever changes to attributes occur, claims are recomputed based on new associated attributes (see section III), allowing immediate access to required mission information. As shown in Figure 4, access control credentials use the Security Assertion Markup Language (SAML) (SAML authorization tokens differ from the more commonly used single-sign-on (SSO) tokens, which in ELS are not used for authentication.) [3]. SAML tokens are signed and the signatures are verified and validated before acceptance. The credentials of the signers also are verified and validated. The credential for access and privilege is bound to the requester by ensuring a match of the distinguished name used in both the authentication and the authorization credentials.

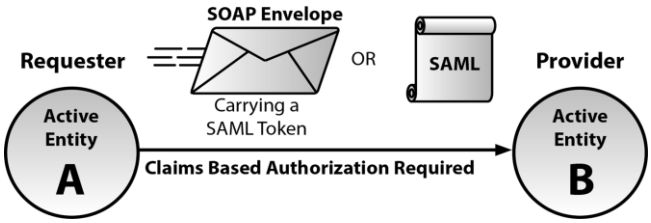

Figure 4: Claims-Based Authorization

D. Maintain Integrity

Integrity is implemented at the connection layer by end-to-end TLS message authentication codes (MACs), see Figure 5. Chained integrity, by which trust is passed on transitively from one entity to another, is not used since it is not as strong as end-to-end integrity. At the application layer, packages (SAML tokens, etc.) are signed, and signatures are verified and validated [4].

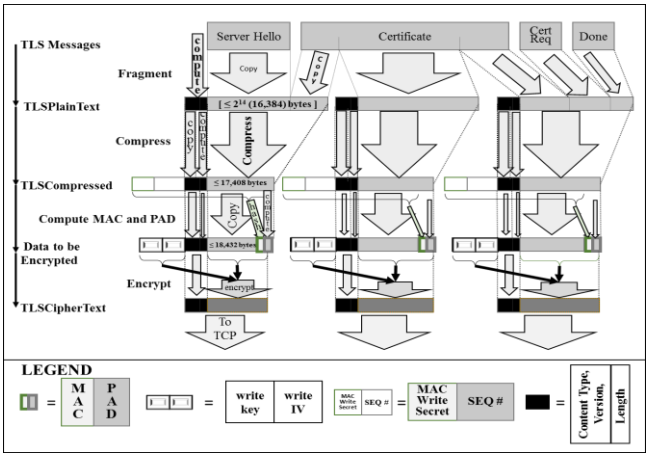

Figure 5: Integrity Measures

E. Require Explicit Accountability

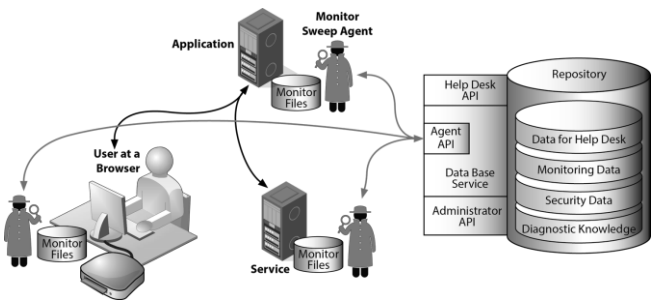

Figure 6: Accountability through Centralized Monitoring

All active entities with ELS are required to act on their own behalf (no proxies, or impersonation allowed). As shown in Figure 6, ELS monitors specified activities for accountability and forensics. The monitor files are formatted in a standard way and stored locally. For enterprise files, a monitor sweep agent reads, translates, cleans, and submits to an enterprise relational database for recording log records periodically or on-demand. Local files

are cleaned periodically to reduce overall storage and to provide a centralized repository for help desk, forensics, and other activities. The details of this activity are provided in designated technical profiles and [5, 6].

In summary, by abiding with the tenets and principles discussed above, ELS allows users access without accounts by computing targeted claims for enterprise applications (using enterprise attribute stores and asset-owner-defined claims for access and privilege). ELS has been shown to be a viable, scalable alternative to current access control schemas [11]. A complete description of ELS basics is provided in [12].

III. IDENTITY ISSUES

Identity in the enterprise is a unique representation of an entity. For users, it begins with the human resources who maintain their files. The assigned identity is called the Distinguished Name (DN) and it must be unique over space and time. There may be five John Smiths in the enterprise, but only one John.Smith2534, UID=Finance, HID=Chicago. These and PKI information are normally encoded into a Personal Identity Verification (PIV) card for network access and provided to the entity for its use. Certain pieces of the information may be tagged as verifiable by DN for identity purposes, such as wife's middle name.

There is a need to allow users without PIVs some degree of access based on alternative authentication methods. PIVs may not be available to all, but also, the user device may not be capable of reading and using a PIV. Additional use cases include lost PIV, waiting for issuance of a PIV, or a user being unable to get a PIV compatible with the ELS certificate authority trust. Additionally, there are federation partners, contractors, and other vetted external individuals with short-term needs.

Each application ultimately decides what kind of authentication is strong enough (through a registration process with Enterprise Attribute Ecosystem (EAE)).

The creation of a non-PIV identity comprises three separate stages. The first stage is creation of a ***proposed identity***. This value is provided by the user. The goal is to correlate this with the enterprise files. It may be an email, a common name, or simply a name. The second stage is creation of a ***candidate identity*** (starting point for identity determination), in which the ***proposed identity*** is paired with an enterprise identity, and a DN is determined. As we will discuss, the process also takes steps to verify that the pairing between the ***proposed identity*** and the DN is owned by the individual making the request. The last stage is creation of the ***assured identity***. The ***candidate identity*** becomes the ***assured identity*** when enough correlated information and personal verification about the ***candidate identity*** has a sufficient level of pairing with the enterprise identity that it can be trusted with access to an application using his/her claims that have been computed for his/her use.

IV. SCALE OF IDENTITY ASSURANCE

If you search the literature for multi-factor authentication, you will find a predominance of processes based upon account-based systems and starting with username–password [13-21]. These systems intertwine the security issues of authentication and authorization. In fact, the popular definition of multi-factor authentication merges the two:

> ***"Multi-factor authentication (MFA) is a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know); possession (something they have), and inherence (something they are)."*** [22]

ELS separates the identity and access/privilege security issues. Thus there are no accounts and no usernames with passwords. Further, ELS uses no proxies and limits access to the enterprise attribute system, thus reducing the threat surface.

Each data owner will decide what the requirements for access and privilege to their data are, and this includes the level of assurance that is acceptable. ELS represents a strong identity assurance and will be assigned a value of .80 (values are arbitrary and subject to revision). It is assumed that if the data owner wishes strong identity assurance he will specify .70 or .75 as the identity assurance value (from the collection below, the value of .75 requires bio information in the absence of PIV). This will allow all enterprise users with a PIV to actually present access and privilege claims to the application. The lowest level of identity assurance would come from self-assertion; however, we will require several additional factors for this minimum, including a presence in the enterprise catalog, verification by an out-of-band (OOB – phone or e-mail) method; and of course for authorization, claims must be available for the individual. This lowest level will be described as User Asserted Identity with OOB verification and assigned a value of .2, which should also be the minimum specified by a data owner. A total of seven identity cases were developed, as follows, with strengths shown in Table 1:

1. Bi-lateral AUTHN (Hard Token) – **AUTHN Hard**
2. Bi-lateral AUTHN (prior issued Soft Token) in protected store. – **ATHN Soft**
3. User Asserted Identity with Out-of-Band (OOB) verification – **OOB**
4. User Asserted Identity with OOB verification and with any Biometric factor – **OOB Bio**
5. User Asserted Identity with OOB verification and with any Biometric factor and with any non-biometric multi-factor verification – **OOB Bio + 1mf.**
6. User Asserted Identity with OOB verification and with any non-biometric multi-factor verification – **OOB + 1mf**
7. User Asserted Identity with OOB verification and with three non-biometric multi-factor verifications – **OOB + 3mf**

Enhanced Identity Assurance:

8. Hard token plus one non-biometric multi-factor verification – **Hard token + 1mf**
9. Hard token plus one biometrics authentication. – **Hard token + 1bio**
10. Hard token plus one biometric and one non-biometric multifactor verification – **Hard token +1bio + 1mf**

Table 1: Multifactor Authentication Identity Assurance

Method	Comment - Strength	Id Assurance
1. AUTHN Hard	Standard ELS –	0.80
2. ATHN Soft	Closest to ELS	0.70
3. OOB	A Start - Minimal	0.25
4. OOB Bio	Solid	0.50
5. OOB Bio + 1mf.	Strong	0.80
6. OOB + 1mf	Moderate	0.60
7. OOB + 3mf	Strong	0.70
Greater than Normal ID Assurance directed by Web Application		
8. Hard token +	Very Strong	0.85
9. Hard token ++	Very Strong	0.90
10. Hard token +++	Highest Value	0.95

V. A TOKEN SERVER WITH CERTIFICATE AUTHORITY

In order to preserve the ELS paradigm, a temporary soft certificate needs to be provided and the user claims must be provided with a SAML credential through TLS. The user needs to be in the attribute system with claims for services sought.

A. Non PIV STS/CA Issued X.509

Non-PIV owners go to a special token server with certificate issuance authority (STS/CA) and provide a ***proposed identity***. This may be email or full name, etc. The STS/CA calls a service that scans the Enterprise Attribute Store (EAS) and rejects any identity that it cannot find in EAS. The STS/CA then confirms that the requester is not an automated system (via Captcha, etc.). This avoids a number of threat vulnerabilities. The STS/CA then asks questions of the non-PIV user to resolve ambiguity (if present). For example, there are five Jon Smiths in the enterprise, but only one works in Finance. The STS/CA then establishes the DN. To this point, the identity is still a ***proposed identity***. The STS/CA saves the DN attributes in separate temporary store and sets up a server side TLS. The next step is a requirement, and non-PIV users must maintain an OOB contact for this. This OOB (one or more) is provided to the human resources for inclusion in the user's enterprise data. The token server resolves OOB (email, phone voice, phone text, etc.) communication methods for DN. We note that OOB means not on the network, and if the enterprise desk phone is part of the enterprise network, it does not work as OOB. Anyone without at least one OOB is rejected.

At this point the token server sends a one-time token (10 minutes or less life) to the OOB and requests input. No input or improper input will be rejected. A successful exchange results in the identity moving to a ***candidate identity***.

The STS/CA will attempt to identify if the user is using a managed device (looking for bio capability like face or fingerprints). The STS/CA retrieves the claims from the enterprise claims store for the established DN, presents a choice from among the services the user has claims to, and asks for a selection. This establishes the application for later SAML transmission. The STS/CA choses the maximum and minimum identify assurance needed for claims. The minimum identity assurance may not be achievable with the device, and a polite rejection is issued if so. Otherwise, the token server begins a multifactor verification, including biological, if applicable. Any multi-level failure leads to exit. If the multi-factor maximum achievable authentication for the identity assurance is successful, the identity becomes an ***assured identity***. The STS/CA then creates and issues a temporary certificate, in the name of the ***assured identity*** DN, and sends this certificate and separately the private key to a specially configured application on the user's device for installation. The temporary certificate contains the identity assurance and has a life of 90 minutes or less. Comments in the temporary certificate, specify the assurance level and the method for the application's use as appropriate. The temporary certificate may be reused for the life of the certificate by selecting any application (this will go to the normal STS for claims).

When the user selects an application, the token server posts a SAML through the browser to the application. The SAML is specifically for the audience (selected application). The temporary certificate is used for authentication to the application, and all else works as with normal ELS for an application. The interaction between the STS/CA and the attribute system is shown in Figure 7.

B. PIV USAGE OF THE STS/CA

A PIV user may be redirected to the STS/CA when the identity assurance requirement for the web application exceeds 0.80. The post will include the identity assurance value of the user (0.80), the identity assurance value sought, and the audience for the multi-factor authentication. The STS will use the user's PIV to authenticate, and the STS/CA will try to increase the identity assurance to the level sought by the application using the methods shown in table 1. It will return a simple "Accomplished" or "No-Go," which is posted back to the application.

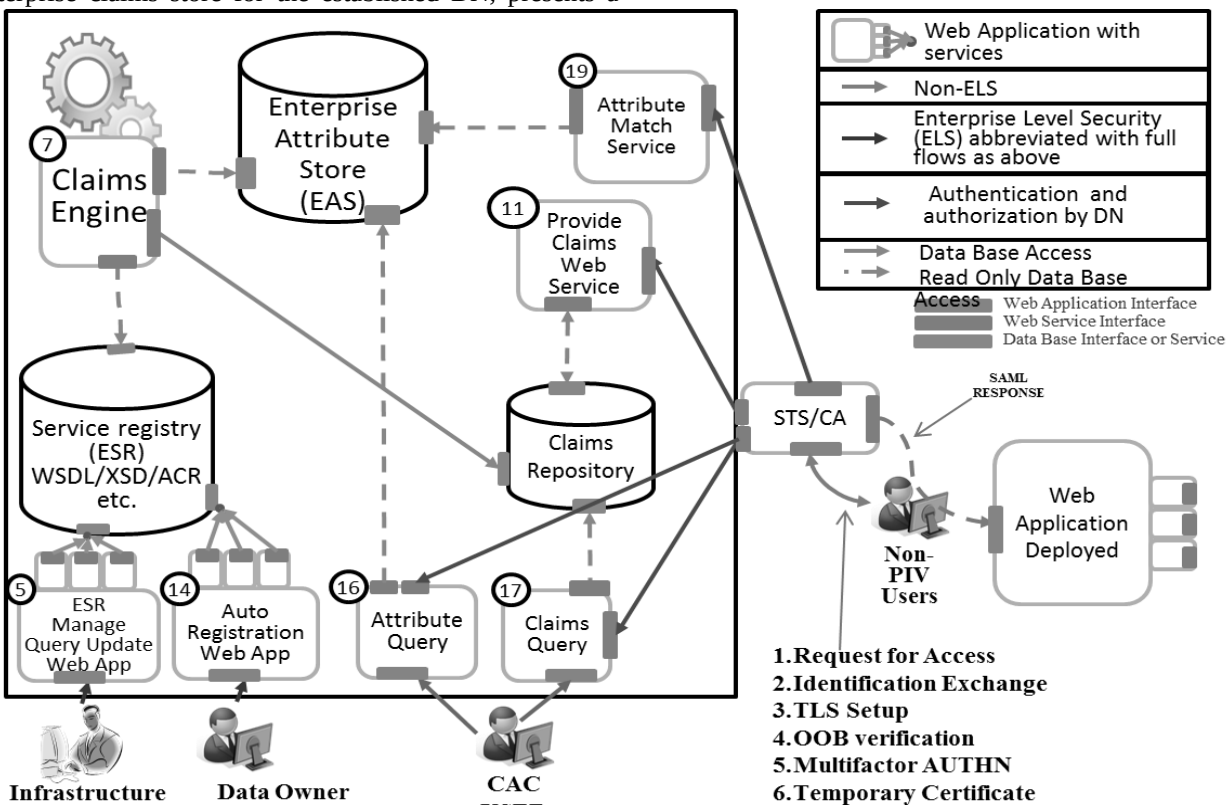

Figure 7: Partial Enterprise Attribute Ecosystem (EAE) for Non-PIV Users and Extended Identity Assurance

VI. REQUIRED ADDITIONAL ELEMENTS

From an ELS standpoint, accommodation of non-PIV users adds the following requirements:

- Data Owners must specify the level of assurance on applications when specifying requirements for access and privilege in the enterprise service registry.
- STS/CA for non-PIV Users needs to be developed.
- An additional service must be placed in the EAE for comparison of attributes in DN retrieval.
- STS/CA must have full crypto and key management capability (generating asymmetric key pairs).
- Device software is needed to install temporary certificates on the end user device.
- The application must recognize temporary certificates generated by the STS/CA (STS/CA must be placed in the trust store).
- The application must recognize SAML certificates provided by the STS/CA.
- The application must check signatures and timestamp, but there is no need for revocation checking of the temporary certificate.

Advantages of the new additions:

- The derived process in this paper is not username/password – there are no accounts and no storage of user data.
- The process will handle retirees, contractors, and temporary employees if they are included in EAS.
- The process will handle missing or forgotten PIV cards.
- Since DN is in EAS claims are computed for each DN in the enterprise stores.
- Claims may be from Delegation (recommend non-PIV cannot delegate)
- All of the ELS software and handlers work without modification.
- The EAS has same attack surface as before.
- Temporary certificates expire out of system quickly.

However, the following disadvantages are noted:

- Only covers person entities (not for Non-Person Entities (NPE) – but an adaption may be possible for NPEs).
- New Vulnerabilities – TBD (i.e., software certificates – short duration is a mitigation).
- Manipulation of identities is possible (OOB requires the threat to have an OOB device in EAS that is really not part of the network).
- The threat's ability to initiate exchange with STS/CA (takes on all comers – reconnaissance by threat entities is facilitated under these circumstances).
- Intercept of temporary credentials (transmission is in TLS – some mitigation).
- On-device recovery of temporary credential (short duration provides mitigation).
- Credential forging (signatures and timeouts are some mitigations).
- The current identity assurance process treats all biometric identifications the same. For future versions, we may wish to distinguish between the types of biometric.
- The current identity assurance process treats all multi-factor queries as the same. For future versions, we may wish to distinguish between the types of multi-factor queries.

VII. SUMMARY

We have reviewed the identity issues in a high-assurance security system. We have also described an approach that relies on high-assurance architectures and the protection elements they provide through PKI. The basic approach becomes compromised when identity is not verified by a strong credential for unique identification (such as holder-of-key in a PKI). The PKI usage is so fundamental to this approach that we have provided non-certificated users a way to obtain a temporary PKI certificate based on their enterprise need and the level of identity assurance needed to provide access and privilege to applications. The process is fully compatible with ELS and works as a complement to existing infrastructure. This work is part of a body of work for high-assurance enterprise computing using web services. Elements of this work are described in [12, 23-36].

REFERENCES

[1] X.509 Standards
   a. DoDI 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 24 May 2011
   b. JTF-GNO CTO 06-02, Tasks for Phase I of PKI Implementation, 17 January 2006
   c. X.509 Certificate Policy for the United States Department of Defense, Version 9.0, 9 February 2005
   d. FPKI-Prof Federal PKI X.509 Certificate and CRL Extensions Profile, Version 6, 12 October 2005
   e. RFC Internet X.509 Public Key Infrastructure: Certification Path Building, 2005
   f. Public Key Cryptography Standard, PKCS #1 v2.2: RSA Cryptography Standard, RSA Laboratories, Oct 27, 2012
   g. PKCS#12 format PKCS #12 v1.0: Personal Information Exchange Syntax Standard, RSA Laboratories, June 1999; http://www.rsa.com/rsalabs/node.asp?id=2138 PKCS 12 Technical Corrigendum 1, RSA laboratories, Feb 2000

[2] TLS family Internet Engineering Task Force (IETF) Standards
   a. RFC 2830 Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security, 2000-05
   b. RFC 3749 Transport Layer Security Protocol Compression Methods, 2004-05
   c. RFC 4279 Pre-Shared Key Ciphersuites for Transport Layer Security (TLS), 2005-12
   d. RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2, 2008-08
   e. RFC 5289 TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), 2008-08
   f. RFC 5929 Channel Bindings for TLS, 2010-07
   g. RFC6358 Additional Master Secret Inputs TLS, 2012-01
   h. RFC 7251 AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS, 2014-06
   i. RFC 7301 Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension, 2014-07
   j. RFC 7457 Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS), 2015-02

[3] Organization for the Advancement of Structured Information Standards (OASIS) open set of Standards
   a. N. Ragouzis et al., Security Assertion Markup Language (SAML) V2.0 Technical Overview, OASIS Committee Draft, March 2008.
   b. P. Mishra et al. Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, March 2005.
   c. S. Cantor et al. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, March 2005.

[4] William List and Rob Melville, IFIP Working Group 11.5, Integrity In Information, Computers and Security, Volume 13, Issue 4, pp. 295–301, Elsevier, doi:10.1016/0167-4048(94)90018-3, 1994.

[5] William R. Simpson and Coimbatore Chandersekaran, CCCT2010, pp. 84–89, "An Agent Based Monitoring System for Web Services," Orlando, FL, Apr 2011.

[6] William R. Simpson and Coimbatore Chandersekaran, 1st International Conference on Design, User Experience, and

Usability, part of the 14th International Conference on Human-Computer Interaction (HCII 2011), "A Multi-Tiered Approach to Enterprise Support Services," 10 pp. Orlando, FL, July 2011. Also published in: A. Marcus (Ed.): Design, User Experience, and Usability, Pt I, HCII 2011, LNCS 6769, pp. 388–397, © Springer-Verlag Berlin Heidelberg 2011.

[7] Technical Profiles for the Consolidated Enterprise IT Baseline, release 3.0. Available at (CAC required) (currently working 4.0): https:// intelshare.intelink.gov/sites/ afceit/TB

[8] Frank Konieczny, Eric Trias and Nevin Taylor, "SEADE: Countering the Futility of Network Security," Air and Space Power Journal, Sep–Oct 2015, Vol 29, No. 5, pg. 4.

[9] Briefing prepared by Accenture Corporation, "USAF Enterprise Level Security, Spiral 5, Codeless Migration of Legacy .NET Applications, High Performance Claims Engine and Performance Test Results," dated 27 September 2013.

[10] Email from Michael Leonard, MITRE Organization on behalf of USAF AFMC ESC/HNCDDD, dated May 10, 2012, Subject: "Performance / Scalability."

[11] Email from Rudy Rihani, Project Manager, Accenture Corporation, dated March 6, 2016, Subject: "manpower savings with ELS."

[12] Simpson, William R., CRC Press, "Enterprise Level Security – Securing Information Systems in an Uncertain World," by Auerbach Publications, ISBN 9781498764452, May 2016, 397 pp.

[13] Sabzevar, Alireza Pirayesh, and Angelos Stavrou. "Universal multi-factor authentication using graphical passwords." Signal Image Technology and Internet Based Systems, 2008. SITIS '08. IEEE International Conference on. IEEE, 2008.

[14] Gordon, Whitson (3 September 2012), "Two-Factor Authentication: The Big List Of Everywhere You Should Enable It Right Now," LifeHacker, Australia. Retrieved 1 November 2012.

[15] Lamport, Leslie, "Password authentication with insecure communication," Communications of the ACM 24.11 (1981), pp. 770–772.

[16] Bauckman, Dena Terry, Nigel Paul Johnson, and David Joseph Robertson, "Multi-Factor Authentication," U.S. Patent No. 20, 130, 055, 368, 28 Feb. 2013.

[17] Bhargav-Spantzel, Abhilasha, et al. "Privacy preserving multifactor authentication with biometrics," Journal of Computer Security 15.5 (2007), pp. 529–560.

[18] Aloul, Fadi, Syed Zahidi, and Wassim El-Hajj, "Two factor authentication using mobile phones," AICCSA 2009, IEEE/ACS International Conference on Computer Systems and Applications, 2009, IEEE, 2009.

[19] The Failure of Two-Factor Authentication (Bruce Schneier, March 2005). https://www.schneier.com/blog/archives/2012/ 02/the_failure_of_2.html

[20] Alzomai, Mohammed, Bander AlFayyadh, and A. Josang, "Display security for online transactions: SMS-based authentication scheme," Internet Technology and Secured Transactions (ICITST), 2010 International Conference.

[21] Liou, Jing-Chiou, and Sujith Bhashyam, "A feasible and cost effective two-factor authentication for online transactions," 2010 2nd International Conference onSoftware Engineering and Data Mining (SEDM), IEEE, 2010.

[22] Multi-factor authentication – Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Multi-factor_authentication

[23] William R. Simpson, Coimbatore Chandersekaran and Andrew Trice, "A Persona-Based Framework for Flexible Delegation and Least Privilege," Electronic Digest of the 2008 System and Software Technology Conference, Las Vegas, Nevada, May 2008.

[24] William R. Simpson, Coimbatore Chandersekaran and Andrew Trice, "Cross-Domain Solutions in an Era of Information Sharing," The 1st International Multi-Conference on Engineering and Technological Innovation: IMET2008, Volume I, Orlando, FL, June 2008, pp. 313–318.

[25] Coimbatore Chandersekaran and William R. Simpson, "The Case for Bi-lateral End-to-End Strong Authentication," World Wide Web Consortium (W3C) Workshop on Security Models for Device APIs, 4 pp., London, England, December 2008.

[26] William R. Simpson and Coimbatore Chandersekaran, "Information Sharing and Federation," The 2nd International Multi-Conf. on Engineering and Technological Innovation: IMETI2009, Volume I, Orlando, FL, July 2009, pp. 300–305.

[27] Coimbatore Chandersekaran and William R. Simpson, "A SAML Framework for Delegation, Attribution and Least Privilege," The 3rd International Multi-Conf. on Engineering and Technological Innovation: IMETI2010, Volume 2, pp. 303–308, Orlando, FL, July 2010.

[28] William R. Simpson and Coimbatore Chandersekaran, "Use Case Based Access Control," The 3rd International Multi-Conference on Engineering and Technological Innovation: IMETI2010, Volume 2, pp. 297–302, Orlando, FL, July 2010.

[29] Coimbatore Chandersekaran and William R. Simpson, "A Model for Delegation Based on Authentication and Authorization," The First International Conference on Computer Science and Information Technology (CCSIT-2011), Springer Verlag Berlin-Heildleberg, Lecture Notes in Computer Science, 20 pp.

[30] William R. Simpson and Coimbatore Chandersekaran, "An Agent Based Monitoring System for Web Services," The 16th International Command and Control Research and Technology Symposium: CCT2011, Volume II, Orlando, FL, April 2011, pp. 84–89.

[31] William R. Simpson and Coimbatore Chandersekaran, "An Agent-Based Web-Services Monitoring System," International Journal of Computer Technology and Application (IJCTA), Vol. 2, No. 9, September 2011, pp. 675–685.

[32] William R. Simpson, Coimbatore Chandersekaran and Ryan Wagner, "High Assurance Challenges for Cloud Computing," Lecture Notes in Engineering and Computer Science: Proceedings World Congress on Engineering and Computer Science 2011, WCECS 2011, San Francisco, USA, 19–21 October 2011, pp. 61–66.

[33] Coimbatore Chandersekaran and William R. Simpson, "Claims-Based Enterprise-Wide Access Control," Lecture Notes in Engineering and Computer Science: Proceedings World Congress on Engineering 2012, WCE 2012, London, U. K., 4-6 July 2012, pp. 524–529.

[34] William R. Simpson and Coimbatore Chandersekaran, "Assured Content Delivery in the Enterprise," Lecture Notes in Engineering and Computer Science: Proceedings World Congress on Engineering 2012, WCE 2012, London, U. K., 4–6 July 2012, pp. 555–560.

[35] William R. Simpson and Coimbatore Chandersekaran, "Enterprise High Assurance Scale-up," Lecture Notes in Engineering and Computer Science: Proceedings World Congress on Engineering and Computer Science 2012, WCECS 2012, San Francisco, USA, 24-26 October 2012, pp. 54–59.

[36] Coimbatore Chandersekaran and William R. Simpson, "A Uniform Claims-Based Access Control for the Enterprise," International Journal of Scientific Computing, Vol. 6, No. 2, December 2012, ISSN: 0973-578X, pp. 1–23.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
11-07-17	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Assured Identity for Enterprise Level Security	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Willliam R. Simpson, Kevin E. Foltz	BC-5-2283
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	NS D-8286 H 2016-001325

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Frank P. Konieczny USAF HQ USAF SAF/CIO A6	SAF/CIO A6
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: William R. Simpson

14. ABSTRACT

Increasing threat intrusions to enterprise computing systems have led to a formulation of guarded enterprise systems. The approach was to put in place steel gates and prevent hostile entities from entering the enterprise domain. The current complexity level has made the fortress approach to security implemented throughout the defense, banking, and other high-trust industries unworkable. The alternative security approach, called Enterprise Level Security (ELS), is the result of a concentrated 14-year program of pilots and research. The primary identity credential for ELS is the PKI certificate, issued to the individual who is provided with a Personal Identity Verification (PIV) card with a hardware chip for storing the private key. All sessions are preceded by a PKI mutual authentication, and a TLS 1.2 communication pipeline is established. This process was deemed to provide a high enough identity assurance to proceed. However, in some instances the PIV card is not available and a compatible approach is needed. This paper discusses a multi-level authentication approach designed to satisfy the level of identity assurance specified by the data owner and to be compatible with the ELS approach for security.

15. SUBJECT TERMS

Identity, Authentication, Multi-Factor Authentication, Enterprise Level Security

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Frank P. Konieczny
Unclassified	Unclassified	Unclassified	Unlimited	6	19b. TELEPHONE NUMBER (Include Area Code) 703-697-1308